EP2790 Säkerhetsanalys av storskaliga datorsystem 7,5 hp

Security Analysis of Large-Scale Computer Systems

Fastställande

Kursplan för EP2790 gäller från och med HT19

Betygsskala

A, B, C, D, E, FX, F

Utbildningsnivå

Avancerad nivå

Huvudområden

Datalogi och datateknik

Särskild behörighet

Slutförd kurs i programmering motsvarande DD1315 Programmeringsteknik och Matlab, DD1316 Programmeringsteknik och C, DD1337 Programmering, ID1018 Programmering I eller motsvarande.

Undervisningsspråk

Undervisningsspråk anges i kurstillfällesinformationen i kurs- och programkatalogen.

Lärandemål

Efter godkänd kurs ska studenten kunna:

- modellera hot i storskaliga datorsystem (inklusive programvara, nätverk, m.m.),
- simulera attacker i storskaliga datorsystem,
- genomföra riskanalys utifrån en modell och simulering,
- beskriva vilka försvarsmekanismer som finns för datorsystem,
- rapportera och presentera modeller, simulering, riskanalys och försvarsstrategi för ett givet system

i syfte att:

- förstå och förklara vilka hot som finns i ett specifikt system,
- förstå och förklara hur attacker går till och propagerar genom en systemarkitektur,
- kunna argumentera för att vissa risker bör prioriteras,
- kunna välja rätt försvar för att minska risk.

Kursinnehåll

Företag idag har tusentals programvarubaserade datorsystem som alla är beroende av varandra i ett stort komplext nätverk, ett system-av-system. Att IT-attacker lyckas i stor utsträckning hänger delvis ihop med denna komplexitet. Ett företag behöver förstå helheten medan en attackerare bara behöver hitta en väg in. Samtidigt finns det en stor mängd attacktyper som utnyttjas och mängder med förslag på försvarsmekanismer. Denna kurs huvudsakliga innehåll syftar till att utveckla studenternas förståelse för:

- dagens komplexa IT-landskap genom att skapa modeller av sådana.
- vilka attacker som idag utnyttjas för att göra skada och hur dessa kan propagera genom ett stort nätverk.
- vilka försvar som finns och när de bäst lämpar sig mot olika attacktyper.
- hur risk kan beräknas och kan användas för att prioritera säkerhetsarbete.

Kurslitteratur

Uppgift om kurslitteratur meddelas i kurs-PM.

Utrustning

Egen dator.

Examination

- PRO1 - Projekt, 6,0 hp, betygsskala: A, B, C, D, E, FX, F

• SEM1 - Seminarier, 1,5 hp, betygsskala: P, F

Examinator beslutar, baserat på rekommendation från KTH:s handläggare av stöd till studenter med funktionsnedsättning, om eventuell anpassad examination för studenter med dokumenterad, varaktig funktionsnedsättning.

Examinator får medge annan examinationsform vid omexamination av enstaka studenter.

När kurs inte längre ges har student möjlighet att examineras under ytterligare två läsår.

Övriga krav för slutbetyg

Examinator beslutar, i samråd med KTH:s samordnare för funktionsnedsättning (Funka), om eventuell anpassad examination för studenter med dokumenterad, varaktig funktionsnedsättning. Examinator får medge annan examinationsform vid omexamination av enstaka studenter.

Etiskt förhållningssätt

- Vid grupparbete har alla i gruppen ansvar för gruppens arbete.
- Vid examination ska varje student ärligt redovisa hjälp som erhållits och källor som använts.
- Vid muntlig examination ska varje student kunna redogöra för hela uppgiften och hela lösningen.